

Updated on 29/11/2023

Sign up

# Calico training: Network management with Kubernetes

2 days (14 hours)

## Presentation

This training course has been specially designed for network teams used to traditional switches, routers and firewalls, to give them the theory and practice to design and operate the network in Kubernetes clusters equipped with the CNI ProjectCalico plugin.

During this course, you'll learn about architectural choices (IPIP/VXLAN encapsulation or bridging, IPAM address management, SNAT masquerading, etc.) for Pod overlay and Node underlay networks, flow distribution mechanisms between Pods (ClusterIP) and how to publish applications (LoadBalancer, NodePort, Ingress).

Increase your skills in controlling and filtering (Network Policy) cluster-internal and external flows, and in interacting (BGP) with the rest of the network.

All participants will have access to an individual cluster (public cloud and bare metal).

The training will be presented with the latest version of Calico, [version 3.24.5](#).

## Objectives

- Understand, design, control, troubleshoot, improve the network in Kubernetes and its interconnection with the "Legacy" world (including BGP)
- Partition namespaces, filter intra- and inter-cluster applications
- Implement micro-segmentation and zero-trust network architecture
- Understand and use Kubernetes' standard and ProjectCalico's open source network functionalities, as well as commercial functionalities.
- Observe network flows

## Target audience

- Legacy network teams
- DevOps

## Prerequisites

Good knowledge of conventional networks (TCP/IP, firewall, proxy, etc.).

## Calico with Kubernetes training program

### Fundamental networking

- Deploy and inspect a clusterip service, then LoadBalancer and NodePort
  - Handling deployments and services
  - Note that Pods obtain @IP dynamically
  - Observe that svcs have stable IPs
- Understanding the network from the pods
  - Learn how to attach a shell to a Pod
  - DNS resolution from the Pod
  - Test TCP intra-cluster connectivity
- Deploy and debug a first application
  - Understanding environment variables
  - Deploy and debug
  - Get an overview of DNS resolution

### Advanced networking

- Source ip preservation with externaltrafficpolicy
  - Understand how external @IPs are modified (i.e. SNAT)
  - Show how externalTrafficPolicy can modify this behavior
- Ebpf and direct server return (DSR)
  - Activate eBPF
  - Detailed analysis of DSR during NodePort access
- Routing and BGP announcements
  - Build in lab a mini Clos matrix (1 spine, 2 leaf)
  - Connect 4 Nodes
  - Enable BGP at node level to broadcast CIDR networks

### Flow filtering

- NameSpace and free circulation
  - Understanding the concept of NameSpace
  - Outgoing and incoming network accesses are independent of the notion of NameSpace

- Writing ingress network policies
  - Writing your first Network Policy Ingress
  - Apply and test
  - View Calico logs
- Partitioning by namespace
  - Writing an Ingress Network Policy to partition Namespaces
  - Apply and test
- Writing egress network policies
  - Writing a Network Policy Egress L3/L4
  - Apply and test
- Flow filtering
  - http - L7: Learn how to build a Calico Network Policy L7
  - Monitor the action of the Envoy (reverse) proxy

## With Calico Cloud/Enterprise

- Network observability
  - Logging
  - Monitoring
  - Network metrics
- Egress Gateway
- WAF (Web Application Firewall) with ModSecurity rule injection

## Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

## Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level on different types of technology, as well as his or her expectations and personal objectives with regard to the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

## Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

## Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

## Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

## Sanction

A certificate will be issued to each trainee who completes the course.